IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1-2, CONTROLLING A COMPUTER NETWORK AND THEREBY INJURING PLAINTIFF AND ITS CUSTOMERS Defendants.	Civil Action No. 1:22-cv-607 (AJT/WEF) **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5**

***EX PARTE* TEMPORARY RESTRAINING ORDER AND**
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.;* (3) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (4) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c)(5) Common Law Trespass to Chattels; (6) Unjust Enrichment; and (7) Conversion. Microsoft has moved *ex parte* for an emergency temporary restraining order and an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C. § 1116(a) (the Lanham Act), and 28 U.S.C. § 1651(a) (the All-Writs Act).

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's *Ex Parle* Application for an Emergency Temporary Restraining

Order and Order to Show Cause re Preliminary Injunction, the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants John Doe 1-2 ("Defendants") under the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §§ 1114, 1125), the common law of trespass to chattels, unjust enrichment and conversion, pursuant to Defendants' breach of contract.

2. Microsoft has made a clear showing that it is likely to succeed on the merits of its claims that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Lanham Act (15 U.S.C. §§ 1114, 1125), and constitute trespass to chattels, unjust enrichment, conversion, and breach of contract, and that Microsoft is, therefore, likely to prevail on the merits of this action;

3. Microsoft owns the registered trademarks Microsoft, Microsoft corporate logo, OneDrive, Share Point and Office 365 and numerous other trademarks used in connection with its services, software and products. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from the Defendants' ongoing violations. The evidence set forth in Microsoft's Brief in Support of *Ex Parte* Application for a Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("TRO Application"), and the accompanying declarations and exhibits, demonstrates that Microsoft is likely to prevail on its claim that Defendants have engaged in violations of the foregoing law by:

a. intentionally accessing and sending malicious software, code, and instructions to the protected computers, operating systems, and computer networks of Microsoft and the customers of Microsoft, without authorization or exceeding authorization, in order to

   i. steal and exfiltrate information from those computers and computer networks;

   ii. infect those computers and computer networks with malicious code and thereby gain control over those computers and computer networks;

   iii. attack and compromise the security of those computers and computer networks by conducting remote reconnaissance, stealing authentication credentials, monitoring the activities of users, and using other instrumentalities of theft;

b. deploying computers, Internet domains and IP addresses to establish a command and control infrastructure by which means Defendants conduct illegal activities, including attacks on computers and networks, monitoring activities of users, and theft of information;

c. corrupting Microsoft's applications on victims' computers and Microsoft's servers, thereby using them to monitor the activities of users and steal information from them;

4. Microsoft has made a clear showing that if such conduct continues, irreparable harm will occur to Microsoft, Microsoft's customers, and the public and that the Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court. In that regard, there is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of command and control software that is hosted at and otherwise operates through the Internet domains listed in **Appendix A** to this Order, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available via those domains, including on user computers infected by Defendants, if Defendants receive advance notice of this action. Based on the evidence cited in Microsoft's TRO Application

and accompanying declarations and exhibits, Microsoft is likely to be able to prove that:

a. Defendants are engaged in activities that directly violate United States law and harm Microsoft and the public, including Microsoft's customers;

b. Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests;

c. Defendants are likely to delete or to relocate the command and control software at issue in Microsoft's TRO Application and the harmful and malicious software disseminated through the Internet domains listed in **Appendix A,** thereby permitting them to continue their illegal acts; and

d. Defendants are likely to warn their associates engaged in such activities if informed of Microsoft's action.

5. Microsoft has made a sufficient showing that the balance of equities strongly favors granting their requested injunctive relief. Defendants can claim no legally cognizable harm because an injunction would only require Defendants to cease illegal activities while failure to grant an injunction would allow Microsoft and its customers to continue to be harmed by Defendants' conduct.

6. Microsoft has made a sufficient showing that granting injunctive relief is in the public interest. Granting injunctive relief would protect additional members of the public from falling victim to Defendants' illegal conduct and having their accounts, computers, and devices unlawfully hacked and their information stolen. Furthermore, the public interest is clearly served by enforcing statutes designed to protect the public

7. Microsoft's request for this emergency *ex parte* relief is not the result of any lack of diligence on Microsoft's part, but instead based upon the nature of Defendants' unlawful conduct. Therefore, in accordance with Fed. R. Civ. P. 65(b), 15 U.S.C. § 1116(a) and 28 U.S.C. § 1651(a), good cause and the interest of justice require that this

Order be Granted without prior notice to Defendants, and accordingly, Microsoft is relieved of the duty to provide Defendants with prior notice of Microsoft's motion.

8. There is good cause to believe that Defendants have operated their spearphishing campaigns through certain instrumentalities - specifically the domains and the domain registration facilities of the domain registries in Virginia identified in **Appendix A.**

9. There is good cause to believe that Defendants have engaged in illegal activity by using the domain registration facilities of the domain registries identified in **Appendix A** to register the Internet domains identified in **Appendix A,** and violated the trademarks of the Microsoft products so as to deceive Microsoft's customers to steal credentials for their Microsoft accounts, and to deliver from those domains the malicious code, content, and commands that Defendants use to access Microsoft's services without authorization and to receive the information stolen from those accounts and computers.

10. There is good cause to believe that Defendants have engaged in illegal activity by using deceptive and fraudulent methods to steal computer users' account credentials and to use such credentials for illegal purposes.

11. There is good cause to believe that to immediately halt the injury caused by Defendants, Defendants must be prohibited from accessing Microsoft's services without authorization and prohibited from sending malicious code, content and commands from the Internet domains identified in **Appendix A** to the computers of Microsoft's customers or to Microsoft's servers.

12. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in **Appendix A** to host the malicious content used to

compromise the computers and servers of Microsoft and Microsoft's customers and to steal information from them. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' domains set forth in **Appendix A** must be immediately transferred beyond the control of Defendants, thus making them inaccessible to Defendants.

13. There is good cause to believe that to immediately halt the injury, the execution of this Order should be carried out in a coordinated manner by Microsoft and by the domain registries identified in **Appendix A** on such date and time within five (5) days of this Order as may be reasonably requested by Microsoft.

14. There is good cause to believe that Defendants may change the Internet domains that they use to conduct illegal activities, and that Microsoft may identify and update the domains listed in **Appendix A** as may be reasonably necessary to account for additional Internet domains associated with Defendants just prior to the execution of this Order and within a reasonable time thereafter should Defendants attempt to evade and defy this Order.

15. There is good cause to permit notice of the instant Order, notice of the Preliminary Injunction hearing and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process, and satisfy Fed. R. Civ. P. 4(t)(3) and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and hosting companies and as agreed to by Defendants in

Defendants' domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE

IT IS THEREFORE ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants, are temporarily restrained and enjoined from: (1) intentionally accessing and sending malicious software or code to Microsoft and the protected computers and operating systems of Microsoft and Microsoft's customers, without authorization, in order to compromise those computers; (2) intentionally attacking and compromising computers or computer networks of Microsoft or Microsoft's customers, to monitor the activities of the owners or users of those computers or computer networks, and to steal information from those computers or networks; (3) configuring, deploying, operating, or otherwise participating in or facilitating infrastructure described in the TRO Application, including but not limited to the software hosted at and operating through the Internet domains set forth in **Appendix A** and through any other component or element of the Defendants' illegal infrastructure at any location; (4) stealing information from Microsoft's customers; (5) misappropriating that which rightfully belongs to Microsoft, its customers, or in which Microsoft or its customers have a proprietary interest; (6) downloading or offering to

download additional malicious software onto the computers of Microsoft's customers; or (7) undertaking any similar activity that inflicts harm on Microsoft, Microsoft's customers, or the public.

IT IS FURTHER ORDERED that, Defendants, Defendants' representatives, and persons who are in active concert or participation with Defendants are temporarily restrained and enjoined from (I) using and infringing Microsoft's trademarks, including specifically Microsoft's registered trademarks Microsoft, Microsoft corporate logo, OneDrive, SharePoint and Office 365 and/or other trademarks, trade names, service marks, or Internet Domain addresses or names containing or infringing such trademarks, trade names or service marks; (2) using in connection with Defendants' activities, products, or services any false or deceptive designation, representation or description of Defendants or of their activities, whether by symbols, words, designs or statements, which would damage or injure Microsoft or give Defendants an unfair competitive advantage or result in deception of consumers; or (3) acting in any other manner which suggests in any way that Defendants' activities, products or services come from or are somehow sponsored by or affiliated with Microsoft, or passing off Defendants' activities, products or services as Microsoft's.

IT IS FURTHER ORDERED that, with respect to any currently registered Internet domains set forth in **Appendix A** to this Order, the domain registries located in the United States shall take the following actions:

A. Within five (5) business days of receipt of this Order, shall unlock and change the registrar of record for the domain to MarkMonitor or such other registrar

specified by Microsoft. To the extent the registrar of record does not assist in changing the registrar of record for the domain under its control, the domain registry for the domain, or its administrators, including backend registry operators or administrators, within five (5) business days of receipt of this Order, shall change, or assist in changing, the registrar of record for the domain to MarkMonitor or such other registrar specified by Microsoft. The purpose of this paragraph is to ensure that Microsoft has control over the hosting and administration of the domain in its registrar account at MarkMonitor or such other registrar specified by Microsoft. Microsoft shall provide to the domain registry or registrar of record any requested registrar information or account details necessary to effectuate the foregoing.

B. The WHOIS registrant, administrative, billing and technical contact and identifying information should be the following, or other information as may be specified by Microsoft:

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052 United States
Phone: +1.4258828080
Facsimile: +1.4259367329
domains@microsoft.com

C. Prevent transfer, modification or deletion of the domain by Defendants and prevent transfer or control of the domain to the account of any party other than Microsoft;

D. Take all steps required to propagate to the foregoing changes through the Domain Name System ("DNS"), including domain registrars.

2. With regard to the domain registries and registrars located outside of the United States, the Court respectfully requests, but does not order, that they take the same or substantially similar actions as the foregoing so as to neutralize the threat posed by the Defendants to the citizens of all countries, including their own. Defendants, their representatives and persons who are in active concert or participation with them are ordered to consent to whatever actions are necessary for non-United States registries, registrars and registrants or hosts, set forth in Appendix A, to effectuate this request.

IT IS FURTHER ORDERED that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) transmission by email, facsimile, mail and/or personal delivery to the contact information provided by Defendants to Defendants' domain registrars and/or hosting companies and as agreed to by Defendants in the domain registration and/or hosting agreements, (2) publishing notice on a publicly available Internet website, (3) by personal delivery upon Defendants, to the extent Defendants provided accurate contact information in the U.S.; and (4) personal delivery through the Hague Convention on Service Abroad or similar treaties upon Defendants, to the extent Defendants provided accurate contact information in foreign countries that are signatories to such treaties.

IT IS FURTHER ORDERED, pursuant to Federal Rule of Civil Procedure 65(b) that a hearing on Microsoft's Motion for a Preliminary Injunction is scheduled for June 10, 2022, at 10:00 am., in which it may request a preliminary injunction pending a final ruling on the Complaint against Defendants, enjoining Defendants from the conduct temporarily restrained by the preceding provisions of this Order.

IT IS FURTHER ORDERED that Microsoft shall post bond in the amount of $15,000 to be paid into the Court registry.

IT IS FURTHER ORDERED that Defendants shall file with the Court and serve on Microsoft's counsel any answering affidavits, pleadings, motions, expert reports or declarations and/or legal memoranda no later than one (1) day prior to the hearing on Microsoft's request for a preliminary injunction.

IT IS SO ORDERED

Entered this 27th day of May, 2022
at 11:30 a.m.

/s/
Anthony J. Trenga
United States District Judge
UNITED STATES DISTRICT JUDGE